

1 Print Access Security System

2
3 FIELD OF THE INVENTION

4
5 This invention is related to security systems and,
6 particularly, to identity recognition through comparison of
7 an image of a finger and a stored template. The security
8 system may be used to gain entry and to energize the systems
9 of a vehicle.

10
11
12 BACKGROUND OF THE INVENTION

13
14 It is generally accepted that vehicles are items
15 considered highly transportable by nature. Vehicles may
16 include cars, trucks, buses, vans, construction equipment,
17 water craft, motorcycles, airplanes, golf carts, snowmobiles,
18 and, generally, anything that is capable of self powered
19 mobility. Common to such vehicles is a key or keys for
20 security of the interior and operation of the systems.
21 However, a key can be used by anyone and is easily
22 duplicated, rendering the security of the vehicle vulnerable
23 to unauthorized use.

24 Some automobile manufacturers utilize different keys for

1 different functions. For instance, General Motors, for many
2 years, employed one key for unlocking the doors and trunk and
3 a second key for starting the engine. However, anyone who
4 had access to the keys would be able to operate the vehicle.
5 More recently, GM has made a key system that includes a
6 microchip. These keys are extremely difficult to duplicate
7 however, there are specialized vendors authorized to make
8 copies. This program also degrades the security system.

9 Other security systems are in use. For instance, Ford
10 Motor Company employs a keyless entry system which allows an
11 individual to have a numeric or alphabetic code programmed
12 into the keyless entry and a memory circuit stores the code
13 for activation of the door locks upon entry of a correct code
14 sequence. The code is typically maintained by the
15 manufacturers as well as the local dealer. Thus, access to
16 the code can be obtained by a number of people thereby
17 degrading the efficacy of the system.

18 Currently, most automobile companies and after market
19 suppliers offer small electronic door openers which cooperate
20 with the electrical system in the auto to unlock doors.
21 These devices are a convenience and may be overridden by a
22 key. As such, these devices do not add any security to the
23 system.

24 In addition to controlling entry to vehicles, there are

1 devices that will cause the engine to start and remotely
2 operate various other electrical systems in the vehicle.
3 However, for security purposes, these devices usually require
4 a key for entry into the vehicle.

5 In both the electronic door locking devices and the
6 electronic engine starters, there is a very real risk that
7 the frequency used in the devices may be captured by
8 unauthorized persons using scanners or like devices. Also,
9 these devices and their associated circuits are over-ridden
10 by the use of the key. Therefore, anyone with the frequency
11 code or a key or both can operate the vehicle.

12 However, what is lacking in the art is a stand alone
13 security system that is hard wired into the vehicle and
14 cannot be duplicated by copying of codes or keys. Further,
15 what is lacking in the prior art is a system that is
16 programmable, only, by the owner or authorized operator of
17 the vehicle without the possibility of unauthorized
18 duplication.

19 Also what is lacking in the prior art is a mechanism for
20 recognizing and verifying less than perfect fingerprint
21 imprints.

1 DESCRIPTION OF THE PRIOR ART

2

3 U. S. Patent No. 5,686,765 to Washington teaches a
4 system for preventing unauthorized or unlicensed persons from
5 using an automobile. In one embodiment, the system has a
6 remote component that receives and compares physiological
7 identification entered at the vehicle. If the data match,
8 the ignition system of the vehicle is energized for normal
9 operation. In another embodiment, the operator data is
10 compared to a particular time frame for operation by that
11 operator during specified times. And in another embodiment,
12 the system requires subsequent data input to ensure that the
13 authorized driver remains the current operator. There is
14 also provision for a bar code reader of an encoded driver's
15 licence and/or reading the signal of an electronic tether.
16 The physiological identification data may be generated by a
17 fingerprint reader or an eyeball scan. This requires a scan
18 and a transmission to a remote computer.

19 U. S. Patent No. 5,448,659 to Hiroshi teaches the use
20 of a card-shaped waveguide-type image transmission device to
21 scan, read and transmit fingerprint data. Again, the
22 identity input is a fingerprint scan.

23 The fingerprint scanning technology of these prior art
24 devices produces a representation of the grooves and ridges

1 of the surface of a finger. Therefore, these scans are
2 highly susceptible to errors caused by extraneous matter such
3 as dirt, grease, paint, calluses, etc. on the fingers of the
4 prospective users.

5
6 SUMMARY OF THE INVENTION

7
8 Accordingly, it is an objective of the instant invention
9 to provide a system to secure any vehicle from operation by
10 an unauthorized user.

11 It is a further objective of the instant invention to
12 provide a system to identify and authenticate a potential
13 user of a vehicle by fingerprint information. The system is
14 referred to as Fingerprint Enrollment and Verification
15 Module, FEVM.

16 It is yet another objective of the instant invention to
17 provide a stand alone system hard wired into the electrical
18 system of a vehicle to authorize and/or control any vehicle
19 function by an operator placing a finger on a sensor.

20 Other objects and advantages of this invention will
21 become apparent from the following description taken in
22 conjunction with the accompanying drawings wherein are set
23 forth, by way of illustration and example, certain
24 embodiments of this invention. The drawings constitute a

1 part of this specification and include exemplary embodiments
2 of the present invention and illustrate various objects and
3 features thereof.

4 5 BRIEF DESCRIPTION OF THE FIGURES

6
7 Figure 1 is a perspective of a door of an automobile;

8 Figure 2 is a close up perspective of the FEVM housing
9 shown in Figure 1; and

10 Figure 3 is a flow chart of the operative steps of the
11 fingerprint enrollment and verification module, FEVM.

12 13 DETAILED DESCRIPTION OF THE INVENTION

14
15 The term, "operation," refers to any initiation of any
16 system on a vehicle, to include a range of commands from
17 merely authorizing a system component to perform in a normal
18 manner to energizing the component to perform. For example
19 and not by way of limitation, authorizing door locks to open
20 with a key or electronic device is an operation. Actually
21 opening the door locks is also an operation. Likewise,
22 authorizing engine start with a key and starting the engine
23 are both operations. Use of any of the subsidiary systems of
24 a vehicle, such as, transmission, radio, air conditioner,

1 convertible top, windless, blade, lights, alarm, and the
2 like, is an operation. The FEVM may be installed to enable
3 or disable any operation of a vehicle.

4 A vehicle, as used in this disclosure, is any mobile
5 conveyance. Most vehicles are self propelled and have an
6 electrical system to operate essential and nonessential
7 components, such as an automobile, truck, boat, airplane,
8 earthmoving equipment, motorcycle, farm equipment including
9 tractors, combines, and military equipment including tanks,
10 self propelled artillery, armored personnel carriers, to name
11 a few. The FEVM is wired into the electrical system of the
12 vehicle to enable or disable the electrically operated
13 components. Of course, the FEVM would be designed to operate
14 on the same electrical current used in the vehicle into which
15 it is to be installed.

16 Vehicles that are not self propelled may be affected by
17 the FEVM blocking the source of power to the vehicle. Also,
18 mechanical components may be enabled or disabled by the FEVM,
19 e.g. by use of solenoids.

20 The FEVM has the capability of storing multiple
21 fingerprint templates so that a number of operators may
22 operate the same vehicle. The FEVM has multiple modes which
23 correspond to different subsystems on the same vehicle and
24 each subsystem may be operated by a different finger of the

1 same operator. For example, a thumb print may unlock the
2 doors of an automobile, an index fingerprint may start the
3 engine, another fingerprint may turn on the cell phone, etc..

4 In Figure 1 an automobile door 10 is shown with a window
5 11, a door handle 12 and a key lock 13. In one embodiment,
6 the FEVM 14 is mounted in an aperture in the door near the
7 door handle. Another embodiment mounts the sensor 18 and the
8 housing 15 in the door with the sensor connected by wiring to
9 the FEVM 14 located in another part of the vehicle. The FEVM
10 may be mounted at any location on the vehicle as a matter of
11 choice. As shown in Figure 2, the FEVM 14 has a housing 15
12 surrounding an aperture in the door (not shown) and connected
13 to the door 10 by screws 16. The housing 15 may be metal or
14 plastic with other connections used, such as welding or
15 adhesives. The housing 15 has an opening 17 of such a shape
16 and size to accommodate the fingerprint of a finger of an
17 operator of the vehicle. A silicone chip sensor 18 is fixed
18 in the housing 15 and extends across the opening 17. The
19 silicone chip is an integral part of a solid state device
20 having an integrated circuit. The sensor surface or matrix
21 contains an active antenna array of more than 16,000 elements
22 and is protected by a hard transparent coating that is
23 scratch and impact resistant. The matrix is surrounded by a
24 drive ring which transmits an extremely small signal that the

1 individual antenna elements can detect. When a finger is
2 placed on the matrix, the drive ring couples a small signal
3 onto the finger's living subdermal layer. The signal is
4 received by the antenna elements which creates a digital or
5 statistical pattern that reflects the finger's unique
6 underlying structure.

7 In operation the FEVM is connected to the print access
8 security system programmer 19. The programmer is connected
9 to the FEVM by plug-in connection. The programmer is powered
10 by the same voltage as the system into which the FEVM is to
11 be installed. The programmer controls the loading function
12 of the FEVM to enroll an operator for operation of a vehicle.

13 The programmer 19 is connected to the FEVM and a mode of
14 operation is chosen, then the operator places a finger on the
15 sensor 18. The enroll function of the programmer is
16 activated by pressing the enroll key. The image of the
17 fingerprint on the sensor 18 is processed by the FEVM to form
18 a template of the fingerprint. The template is not a picture
19 or representation of the actual grooves and ridges of a
20 fingerprint. The template is statistical information about
21 the fingerprint image and may be 144 bytes in length. As
22 such, the FEVM does not require a pristine fingerprint to be
23 enrolled but may successfully complete the function when the
24 fingerprint image includes extraneous material, such as

1 perspiration, dirt, paint or grease. When the template is
2 complete, it is stored in the flash memory to complete the
3 enrollment function. An indicator will signal the end of
4 this function. The operator removes his finger from the
5 sensor.

6 The operator then places the same finger on the sensor a
7 second time and the verify key on the programmer is
8 activated. The FEVM compares the image on the sensor to the
9 template stored in the memory. A signal, such as a green
10 light, will indicate that the image and the template match.
11 The operator is now an authorized user of the mode for which
12 he is verified on the vehicle.

13 This procedure is repeated for each operator and each
14 mode until complete. The programmer 19 is then unplugged
15 from the FEVM and stored in a secure location. At this
16 point, the FEVM is fully programmed with no electrical or
17 electronic vulnerability. Any physical tampering with the
18 FEVM would merely disable the hardware without invading the
19 software.

20 Figure 3 illustrates the steps for opening a door lock
21 using the FEVM. The prospective operator places a finger on
22 the passive sensor 18, the sensor activates and detects the
23 presence of the finger, the fingerprint image is compared to
24 the templates in the flash memory to verify the prospective

1 user. If there is no verification, ie. no match in the
2 memory for the prospective operator, the sensor returns to
3 the detect step. If there is a verification and the
4 fingerprint image has a template in the memory, the door
5 unlocks. The finger is removed and the sensor returns to the
6 passive mode.

7 When the authorized user leaves the car, he again places
8 his finger on the sensor and the doors lock.

9 A detailed command description of the FEVM follow:

10 Standalone Fingerprint

11 Enrollment

12 and

13 Verification

14 Module

15 (FEVM)

16 Rev 1.0

17 October 28, 2000

18 **Table of Contents**

19 PRINT ACCESS Fingerprint Enrollment and Verification Module

20 Host Interface Command Set

21 Command Summary

22 Basic Concepts

23 Detailed Command Description

24 Status

25 Enroll

26 Verify Parameters

27 Verify

1 the Print Access Security
2 model of Fingerprint Enrollment and Verification Modules.
3 Using these commands, all functionality of the Print Access
4 Security module is exposed to the host CPU. The
5 commands are simple single byte op-codes that are issued
6 through the RS-232 interface. There are two types of
7 commands; immediate and long. Immediate commands return
8 their results immediately. Long commands require an extended
9 length of time to
10 complete. The device status should be polled to determine
11 when such a command has completed or failed.
12
13
14

15 Command Summary

16
17 Command Op-code Description Status Ox00Retrieve the 2 byte
18 device
19 statusEnroll0x01Generate an enrollment template from a
20 finger-Verify0x02Verify a finger against an enrollment
21 template(s)Baud0x03 Set the RS-232 baud rateUpload0x04Send
22 the active enrollment template to the
23 hostDownload0x05Download an enrollment template
24 from host and activateImage0x06Send the enroll Fingerprint
25 image to the
26 hostStore0x07Store the active enroll template in the
27 deviceRetrieve0x08Retrieve an
28 enroll template from the device and activateHeader0x09Return
29 the header from a stored templateSignature0x0AReturn the
30 device signature GEZ6xxrrrErase0x0BErase the
31 specified stored templatePersistent0x0CMake the current
32 settings persistentCalibrate0x0DCalibrate the
33 devicePrivilege0x0EBegin access to privileged
34 commandsRestrict0x0FEnd access to privileged
35 commandsSetCode0x10Set a new
36 privilege codeVerifyParameters0x11Set the verification
37 parameters
38
39

40 Basic Concepts

41
42 The basic operation of the FEVM is the Enrollment and
43 Verification of fingerprints. All additional functionality is
44 simply in support of these two key operations.
45

46 Enrollment is a process by which a fingerprint image captured
47 by the sensor is transformed into a template. A template may

1 be up to 144 bytes in length and contains statistical
2 information about a particular fingerprint image. This
3 information is
4 sufficient to perform verification when the same -finger is
5 again placed on the sensor. The template is not a fingerprint
6 image.

7
8 Verification is a process that applies the statistical
9 information found in an enrolled template against a
10 fingerprint image currently captured by the sensor- No
11 fingerprint image is transmitted outside of the FEVM during
12 verification.

13
14
15 Active Enrollment Buffer: The active enrollment buffer is
16 used to hold an enrollment template. After enrollment it
17 contains the template that has just been enrolled. Prior to
18 verification it should be loaded with the template to be
19 verified. Store and Upload use this Buffer as a source
20 whereas Download and Retrieve use this buffer as a
21 destination.

22
23 Storage Slot: A Storage slot is a piece of Flash memory
24 allocated within the FEVM to hold enrolled templates.
25 Enrolled templates may be stored, retrieved or erased from a
26 storage slot.

27 Detailed Command Description

28
29 Status

30
31 Op-code: 00H
32 Type: Immediate
33 Parameters: None
34 Returns:

35 Byte 1: Command Status

36
37 The bits are described in the following table:

38 **BitMeaning**0St Fail: Previous command failed if
39 set.

40 1StInEnroll: Performing Enrollment if set.

41 2StInVerify: Performing Verification if set.

42 3StInStore: Storing data in Flash Memory if set.

43 4StInCalibrate: Calibrating if set.

44 6StPermission: Insufficient permissions.

45 7StFinger: A finger is placed on the device if set.

46 Byte 2: Extended Status

47 The extended status byte provides extra status
48 information for a command. This information is command and

context dependent.

CommandMeaning Verify If Bit 0 is set during verification, then the FEVM is performing verification against the internal storage slots. If Bit 0 is clear during verification, then the FEVM is performing verification against the Active Enrollment Buffer. If verification of multiple storage slots has completed then this status byte contains the verified storage slot number if the verification was successful.

-Enroll During enrollment, the bits for this status byte are defined as follows, Bit Meaning 0 The finger pressure needs adjusting if set. See bits 1 and 2 for pressure direction. The yellow LED will be on plus one of the green or red LEDs. 1 If bit 0 is set then too much finger pressure is being applied to the sensor. If bit 0 is cleared then the finger is positioned too far to the left of the sensor. The red LED will be on. (Orientation: LEDs are at the top) 2 If bit 0 is set then too little finger pressure is being applied to the sensor. If bit 0 is clear then the finger is positioned too far to the right of the sensor. The green LED will be on.

Description

Returns the current status of the device. This command may be invoked at any time.

Enroll

Op-code: 01H

Type: Long

Parameters: None

Returns: None

Description:

Initiates enrollment. The command does not complete until a successful enrollment has been achieved. To abort this command the device must be reset. To check for completion of this command, the Status must be polled. The StInEnroll bit will be cleared when this command completes. The host may detect when an individual has placed their finger on the sensor of the device by checking the StFinger bit.

VerifyParameters

Op-code: 11H

Type: Immediate

Parameters:

1 Byte 1: The storage slot to begin verification from,
2 Byte 2: The number of storage slots to verify. If
3 this byte is 0 then verification is performed on the active
4 enrollment buffer.

5
6 Returns: None.

7 8 **Description:**

9 This command sunply sets the Verification parameters.
10 Separating the parameters from the Verify command is useful
11 when configuring FEW4s. An application may wish to
12 store multiple templates on an FEVM and then configure it to
13 perform verification on these templates. Forcing verification
14 is not necessary. E.g. enrolling an individual from a hotel
15 lobby and programming their door lock remotely.

16
17 Note: To make these parameters persistent, the Persistent
18 command should be called
19 prior to the next invocation of reset, The Factory defaults
20 are 0,0.

21 22 **Verify**

23 Op-code: 02H

24 Type: Long

25 Parameters: None. The parameters are set using the
26 VenfyParameters command.

27 Returns: None.

28 29 **Description:**

30 Initiates verification. The command does not complete until a
31 successful verification has been achieved. To abort this
32 command the device must be reset. To check for the
33 completion of this command, the Status must be polled. The
34 StInVerify bit in the first status byte will be cleared when
35 verification has completed. The host may detect when an
36 individual has placed a finger on the sensor of the device by
37 checking the StFinger bit. The second status byte may be used
38 to detect if a multiple verification or an Active Enrollment
39 Buffer verification is taking place.

40 41 **Baud**

42 Op-code: 03H

43 Type: Immediate

44 Parameters: Byte 1: The new baud rate to be set. Supported
45 Baud rates are as follows:

46 47 **Baud**

RateValue1200024001480029600314,400419,200528,800638,400757,
6008115,2009
Returns: None.

Description:

Change the communication baud rate for the device to the newly supplied baud rate.

Note: To make the new baud rate persistent, the Persistent command should be called prior to the next invocation of reset The factory default is 3 (9600 baud).

Upload

Op-code: 04H

Type: Immediate

Parameters: None.

Returns: The currently enrolled template in the active enroll buffer. The actual size of the template must be determined by examining the header of the template. The header is the first 2 bytes of the data being returned.

Template Header

BitsDescription0-1Reserved2-3The template structure4-6Template types: 3=84 bytes,4=104 bytes,6=144 bytes Sizes include the header and trailer.7Valid template if clear. Invalid (deleted)if set.8-15Reserved for user data

Description:

Upload the template in the active enrollment buffer to the host.

Download

Op-code. 05H

Type: Immediate

Parameters: A valid template that has been previously uploaded from the device. The size of the download template is determined from the header. (See Upload)

Returns: None. The device status should be checked for failure status.

Description:

Download a template from the host and store it in the active enrollment buffer. This makes the template available for verification, storage or Upload.

Image

Op-code: 06H

Type: Immediate

Parameters: None

Returns:

Byte 1: The image type id.

0: No image.

1: The next 2 bytes contain the width and height.

Byte 2: The width of the enrollment image in pixels

Byte 3: The height of the enrollment image in pixels

Subsequent Bytes: The enrollment image. This is a black and white image with a bit depth of one.

Description:

This image may be used to visually inspect the image of the finger that was just enrolled- The most unique features of the finger should be in the center of the image. A good enrollment is necessary for easy verification. This visual inspection is not necessary for enrollment but makes enrollment simpler. An alternative may be to enroll and then verify several times to ensure the quality of the enrolled image.

Store

Op-code: 07H

Type: Long

Parameters:

Bytel: The internal FEVM slot number to be used to store the active enrollment template. This number must be between 0 and 63.

Returns: None. To check for success or failure of this command, the device status must be polled. Once the StInStore bit has been cleared from the first status byte, the Failed bit will indicate success or failure of this command.

Retrieve

Op-code: 08H

Type: Immediate

Parameters:

Bytel: The internal FEVM slot number of the enrollment template to be retrieved. This number must be between 0 and 63.

Returns: None. This is an immediate command. The status byte should be checked to determine success or failure.

1 **Description:** Retrieve the stored template and place it in the
2 active enrollment buffer. This makes the template available
3 for Verify, Upload or Store.
4

5 **Header**

6 Op-code: 09H

7 Type: Immediate

8 Parameters:

9 Bytel: The internal FEVM slot number of the
10 enrollment template to be retrieved. This number must be
11 between 0 and 63.
12

13 Returns: The 2 byte header from the stored template. Refer to
14 the Upload command for a description of the header.
15

16 **Description:**

17 This command is used to recover the header from a
18 stored template. This is useful for applications that may be
19 using the user data component of the header and wish to
20 search through the stored templates to recover this data.
21

22 **Signature**

23 Op-code: 0AH

24 Type: Immediate

25 Parameters: None.

26 Returns: A string representing the signature of the
27 device. The expected return value is "GEZxxxxrrr" where "xxx"
28 represents the model of the module and rrr represents the
29 revision. E.g "GEZ6Aa001" where 6Aa is the model and 001 is
30 the revision.
31

32 **Description:** Returns a device signature string. This
33 command also unlocks the FEVM command engine and must be
34 issued after a reset or power on.
35

36 **Erase**

37 Op-code: 0BH

38 Type;Long

39 Parameters:

40 Bytel: The internal FEVM slot number of the
41 enrollment template to be erased. This number must be between
42 0 and 63.
43

44 Returns: None. The status of the device should be polled
45 to determine the success or failure of this command. The
46 StInStore bit will be cleared when the command has completed.
47

1 **Description:** Erase the enrolled template stored in the FEVM at
2 the given slot number.
3
4

5 **Persistent**

6 Op-code: OCH

7 Type: Long

8 Parameters: To help eliminate the possible accidental
9 invocation of this command, the command accepts the op-code
10 (OCH) as the one-byte parameter.
11

12 **Returns:** None. The device status should be polled to
13 determine the success or failure of this command. The
14 StInStore bit will be cleared when the command has completed.
15

16 **Description:** This command will make the current
17 calibration, verification, baud rate and Privilege code
18 settings persistent.
19

20 **Calibrate**

21 Op-code: ODH

22 Type: Long

23 Parameters: None.

24 Returns: None. The device status should be polled to
25 determine when the calibration has finished. The
26 StInCalibrate bit will be cleared when the command has
27 completed. The newly calibrated values will be made
28 persistent if the Persistent command is invoked.
29

30 **Description:** This command will cause the FEVM to perform
31 calibration. No finger should be present on the FEVM sensor
32 when calibration is being performed.
33

34 Note: To make this calibration persistent, the Persistent
35 command should be invoked prior to the next reset.
36

37 **Privileges**

38 Op-code: OEH

39 Type: Immediate

40 Parameters: The Privilege code. This is the code previously
41 set using SetCode. It is 6 bytes long. If a Privilege code
42 has never been set for this device, then the parameter must
43 be set but is ignored.
44

45 Returns: None. The device status should be polled to
46 determine if privileges have been granted. The StPrivilege
47 and StFail bits in the status word will be set

1 if the privilege code was invalid-

2
3 **Description:** If the privilege code that is given matches the
4 privilege code that is currently stored in the FEVM, then
5 permission is granted to perform Image, Download, Persistent,
6 Enroll, Store and Erase.

7
8 Note: If no privilege code has been previously set then all
9 privileges are granted without the necessity of calling the
10 Privilege command.

11 12 13 **Restrict**

14
15 Op-code: OFH
16 Type: Immediate
17 Parameters: None.
18 Returns: None.

19
20 **Description:** If privileges are currently active, then this
21 commands disables access to privileged operations thereby
22 disabling Image, Download, Persistent, Enroll, Store and
23 Erase.

24
25 Note: If the Privilege code has been made persistent then
26 resetting the device will have the same effect as calling
27 Restrict

28 29 **SetCode**

30 Op-code: 10H
31 Type: Immediate
32 Parameters: First 6 bytes: The currently set Privilege code.
33 If no privilege code currently exists, then this parameter
34 should contain 6 bytes of zeroes.
35 Next 6 bytes: The new Privilege code.

36
37 **Description:** Sets a Privilege code for the FEW This privilege
38 code is used with the Privilege command and is used to
39 control access to Image, Download, Persistent, Enroll, Store
40 and Erase.

41
42 Note: To make new Privilege code persistent, the Persistent
43 command should be called prior to the next invocation of
44 reset. The factory default is 0x000000000000.

45
46 Serial Interface Command Features
47

Power On/Off

To power the device off, bring the DTR signal low (0). This will cause power to the device to be dropped down to nominal levels and prevent it from functioning. Bringing DTR high (1) will cause the device to resume operation. All non-persistent setting will have been lost and must be reprogrammed.

Reset

To reset the device, simply toggle the power off and back on using DTR as described above. A delay should be added after power on before the device is fully functional. This delay is approximately 200 ms.

Hardware Signals and Connections

The fingerprint module interface connectors are located on the back of the module (see FIG. 1). Viewing the module from the backside, with the connectors on the top edge, the STANDALONE connector will be on your right side, and the SERIAL connector is on the left side. The connectors are manufactured by Hirose Electric and belong to the FH12 series of 0.5mm-pitch flex-cable connectors. An appropriate cable to use with these connectors would be Parlex Corporation part#0.5MM-10-2-B.

CAUTION. All module input signals are rated at 3.3 volts, and they are NOT 5 volt tolerant. All module output signals must be buffered if they are required to drive LEDs, etc.

Standalone Connector

The standalone connector allows the FEVM to operate without an additional micro controller. A serial interface will still be required to program the FEVM with templates, Privilege code and verify parameters.

Standalone Connector

PIN	#	PIN	NAME	DIRECTION	FUNCTION
1	5	1	VCC5V	INPUT	5Volt supply
2	2	2	GND	power/signal	ground
3	3	3	GND	power/signal	ground
4	4	4	CTRL-OUT	OUTPUT	Active low output indicating verification successful.
5	9	5	OUT	PUT	Yellow LED active low output.
6	7	6	OUT	PUT	Red LED active low output.
7	6	7	OUT	PUT	Green LED active low output.
8	4	8	IN	PUT	ENROLL user switch control - active low
9	5	9	PB5		

1 -INPUTVERIFY user switch control - active low I⁰INTA-
2 INPUTSTART user switch control - active low (shared with BOOT
3 mode control - DO NOT use during DSP boot sequence.)** all
4 signal directions are with respect to the fingerprint module
5 (ie. INPUT indicates input for the module)
6

7 CAUTION: All module input signals are rated at 3.3 volts, and
8 they are NOT 5 volt tolerant. All module output signals must.
9 be buffered if they are required to drive LEDs, etc.

10 11 Functional Description of I/O Signals:

12
13 To perform enrollment using the Standalone Connector:

- 14 • PB₄ should be brought low for at least 20 ms then
15 returned to high. The green LED will be on.
- 16 • PB₅ should be brought low for at least 20 ms then
17 returned to high- The green LED will be off
- 18 • The device will be in enrollment mode. (No LEDs are
19 on)
- 20 • Place a finger on the sensor.
- 21 • If PB₇ (red LED on) is low and PB₉ (yellow LED is
22 off) is high then the finger placed is too far to the left.
- 23 • If PB₆ (green LED on) is low and PB₉ (yellow LED is
24 off) is high then the finger placed is too far to the right.
- 25 • If PB₇ is low and PB₉ is low then too much pressure
26 is being applied to the sensor (or the finger is too moist).
- 27 • If PB₆ is low and PB₉ is low then too little
28 pressure is being applied to the sensor.
- 29 • Upon successful enrollment PB₆ and PB₇ are high and
30 PB₉ is low (yellow LED is on).

31
32 To perform verification using the Standalone Connector:

- 33 • PB₅ should be brought low for at least 20 ms then
34 returned to high.
- 35 • The device will be in verification mode.
- 36 • When verification is successful, CTRL - OUT will be
37 made high, otherwise it will remain low. (Future
38 implementation) The green LED will be on.

39
40
41 To cancel either enrollment or verification, INTA should
42 be brought low for at least 20 ms and then returned to high-
43 This will effectively reset all device parameters and return
44 it to monitor mode.

45 46 Serial Connector

47 The serial connector is used to interface the FEVM with an
48 external CPU. This CPU has access to all the FEVM

1 functionality.

2
3 Serial Connector **PIN#PIN NAME DIRECTION**FUNCTION**1VCC5VINPUT5
4 volt
5 supply2VCC5VINPUT5 volt supply3GND-power/signal ground4GND-
6 power/signal
7 ground5GND-power/signal ground6CTS-INPUT(reserved)
8 Functionality will change in
9 future revisions. 7RTS-OUTPUT(reserved) Functionality will
10 change future revisions. 8RXINPUTRS-232 serial data
11 input.9TXOUTPUTRS-232 serial data
12 output. 10SYS-RESET-INPUTModule reset/power-down. Active
13 low.** all signal directions are with respect to the
14 fingerprint module (ie. INPUT indicates input for the module)
15

16 CAUTION: All module input signals are rated at 3.3 volts, and
17 they are NOT 5 volt tolerant. All module output signals must
18 be buffered if they are required to drive LEDs, etc.
19

20 It is to be understood that while a certain form of the
21 invention is illustrated, it is not to be limited to the
22 specific form or arrangement of parts herein described and
23 shown. It will be apparent to those skilled in the art that
24 various changes may be made without departing from the scope
25 of the invention and the invention is not to be considered
26 limited to what is shown and described in the specification
27 and drawings.
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48